

In the claims:

Cancel claims 4-6.

Amend claims 1-3, 7-9, 11, and 13 as shown in the marked-up version of the claims in the Appendix.

Add new claims 14-41.

REMARKS:

The parenthetical "(encryption)" is added to paragraph 5 of the specification to clarify the fact that a private key used for encrypting data is an encryption key. Clarification appears to be necessary to bring to the reader's attention that there are at least two types of private keys, encryption keys and decryption keys, that perform substantially different and even diametrically opposed functions. Use of the key for the purposes of encryption was previously discussed, for example, on page 5 line 20 and even characterized as an "encryption key" on page 7 line 19. This modification therefore does not add new matter to the specification.

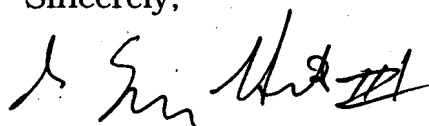
The second change to paragraph 5 clarifies that "other types of biometric readings" are obtained from types of biometric readers other than fingerprint scanner 108, as implied by the use of the word "other." This modification, therefore, does not introduce new matter.

The amendment to the summary is introduced for the same reasons as the first modification requested for page 5 and does not introduce new matter for the reasons discussed above.

A replacement specification reflecting the above amendments is provided in this communication. Paragraph numbers have been added to the specification to conform with current practice.

The preceeding amendments are made to clarify the invention and do not add new matter to the specification.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Eppa Hite', with a stylized flourish at the end.

J. Eppa Hite
Reg. No. 30,266
Carr & Ferrell LLC
Suite 200
2225 East Bayshore Rd.
Palo Alto, CA 94303
(650) 812-3428
eppa@carr-ferrell.com

00/554,518

2131

APPENDIX

Marked-up version of Specification and Claims as-filed showing
changes made in substitute Specification and Claims.



SYSTEM AND METHOD OF AUTHENTICATING A KEY AND TRANSMITTING SECURE DATA

Lynn D. Spraggs

RECEIVED
AUG 24 2001
Technology Center 2100

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0001] The present invention relates generally to computer security and more specifically to allow the authentication of a key for the transmission of secure data between computers using the key.

DESCRIPTION OF THE PRIOR ART

[0002] In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

[0003] A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

[0004] In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority. The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

[0005] The private key is vital key to a user. If the private key is copied or stolen from the user, then secured data can be compromised as well as causing problems in properly authenticating the private key and the user using the private key.

[0006] Thus, it would be desirable to provide a system and method of authenticating a key so that the transmission of secure data using the key can be reliably originating from an authenticated key and/or an identifiable user.

SUMMARY OF THE INVENTION

[0007] A system and method is provided for authenticating an encryption key of a user by decrypting an encrypted data file provided by the user with a password provided by the user into the authenticated encryption key of the user. The encrypted data file can be stored on a RF smart card and can contain encrypted biometric data identifying the user, such as a fingerprint. An additional security measure can be used by taking a digitized biometric fingerprint scan of the user and probabilistically comparing the digitized fingerprint scan of the user with the authenticated key of the user. The user's key can then be used to securely encrypt and transmit data accordingly knowing that the key has been authenticated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a user's key being authenticated prior to transmitting secure data over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the client computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the client computer of FIG. 2; and

FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer, according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0009] The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

[0010] Referring now to FIG. 1, a schematic diagram illustrates a web server 100 and a client computer 102 connected to the Internet 110. For security purposes, the client computer 102 has a RF reader (radio frequency reader) 104 for reading a RF smart card 106 having a user's private (encryption) key. The private key on the RF smart card 106 can be very long (i.e.g. 1000 bytes) and could include any type of biometric data, such as a digitized fingerprint of the user. The private key could be very long and any data that is encrypted using this private key would be virtually impossible to decrypt by a hacker, since this private key can be much longer than a typical private key (64 bytes) used in a

private/public key system. The client 102 also has a fingerprint scanner 108 for helping to authenticate the private key of the user. Biometric readings employed by this invention are not limited to fingerprints.

Other types of biometric readings, obtained from other types of biometric readers, can also be used, such as the reading from the eye and analysis of the face.

[0011] FIG. 2 is a block diagram of the client computer 102 shown in FIG. 1. Computer 102 includes a CPU 202, a RAM 204, a non-volatile memory 206, an input device 208, a display 210, an Internet interface 212 for providing access to the Internet, a RF reader interface 214, and a fingerprint scanner interface 216.

[0012] FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the client computer 102 of FIG. 2. The non-volatile memory 206 includes an encrypt/decrypt engine 302 for encrypting and decrypting data.

[0013] The encrypt/decrypt engine 302 is programmed to encrypt and decrypt data using a password or a key. Excellent results can be obtained when using the blowfish algorithm for encryption and decryption. Other types of symmetric key encryption/decryption algorithms can also be employed within the encrypt/decrypt engine 302.

[0014] FIG. 4 is a flowchart of a method illustrating the authentication of a key at a client computer in accordance with the invention. The authentication process begins at step 400. The authentication process

includes three security levels, however, not every level of security is required to authenticate the key of the user. Depending on the type of application, only one or two of the security levels may be employed.

[0015] Security level I 402 begins at step 404 where the user scans his user's RF key card 106 with the RF reader 104. Security level II 406 then begins at step 408 where the user enters his password at the client computer 102. At step 410 the data scanned from the user's RF key card is decrypted with the encrypt/decrypt engine 302 using the user's password.

[0016] At step 414, security level III 412 begins and a digitized fingerprint scan is taken from the user. At step 416 the digitized fingerprint scan is compared with the data decrypted from the RF key card. At step 418 it is determined if there is a probabilistic match between the digitized fingerprint scan and the data decrypted from the RF key card. If it is determined that there is not a match, then at step 420 the authentication of the user's key fails and is rejected. If at step 418 it is determined that there is a match, then at step 422 the user's key is authenticated. The decrypted data from the RF key card can then be used as an authenticated encryption key for sending data to a server over and unsecure network, such as the Internet.

Version of claims showing changes.

I Claim:

1. (Amended) A system for authenticating an encryption key of a user, comprising: a decrypt engine for using a password provided by the user to decrypting an encrypted data file provided by the user ~~with a password provided by the user into the~~ encryption key of the user.
2. (Amended) The system of claim 1, wherein the encrypted data file is stored on an RF smart card.
3. (Amended) The system of claim 1, wherein the encrypted data file includes ~~contains~~ encrypted biometric data identifying the user.
7. (Amended) A method for providing an authenticated encryption key of a user, comprising the steps of:
 - providing an encrypted data file;
 - providing a password; and
 - decrypting the encrypted data file, using the password, into an authenticated encryption key of the user.

1 8. (Amended) The method of claim 7, wherein the encrypted data
2 file is stored on an a-RF smart card.

1 9. (Amended) The method of claim 7, wherein the encrypted data
2 file ~~contains~~ includes encrypted biometric data identifying the user.

1 10. The method of claim 9, wherein the biometric data includes a
2 digitized fingerprint of the user.

1 11. (Amended) The method of claim 9, further including the steps
2 of:

3 generating biometric data of the user by scanning a biometric
4 feature of the user; and

5 probabilistically comparing the scanned biometric
6 feature generated biometric data of the user to data derived from the
7 encrypted data file with the key of the user in order to additionally
8 authenticate the encryption key of the user prior to securely
9 transmitting data using the key.

1 12. The method of claim 11, wherein the scanned biometric feature
2 of the user is a fingerprint.

1 13. (Amended) A computer-readable-accessible medium comprising
2 program instructions for providing an authenticated encryption key of
3 a user, by performing the step of:
4 using a password provided by the user to decrypt decrypting an
5 encrypted data file provided by the user using a password provided by
6 the user into an authenticated encryption key of the user.

1 14. (New) The system of claim 1, wherein the encrypted data file
2 includes encrypted biometric data, derived from a digitized fingerprint
3 of the user, identifying the user.

1 15. (New) The system of claim 1, further comprising a biometric
2 reader for generating a first biometric data of the user, wherein the
3 first biometric data of the user is compared with a second biometric
4 data of the user stored in the encrypted data file.

1 16. (New) The system of claim 1, further comprising a fingerprint
2 scanner for generating a first digitized fingerprint of the user, wherein
3 the first digitized fingerprint of the user is compared with a second
4 digitized fingerprint of the user stored in the encrypted data file.

1 17. (New) A system for authenticating an encryption key of a user,
2 comprising:
3 _____ an input device for receiving a password provided by the user;
4 _____ memory for storing an encrypted data file including an
5 encryption key of the user; and
6 _____ a decrypt engine for using the password to decrypt the
7 encrypted data file and thereby generating an authenticated
8 encryption key of the user.

1 18. (New) The system of claim 17, wherein the encrypted data file is
2 stored on an RF smart card.

1 19. (New) The system of claim 17, wherein the encrypted data file
2 includes encrypted biometric data identifying the user.

1 20. (New) The system of claim 17, wherein the encrypted data file
2 includes encrypted biometric data, derived from a digitized fingerprint
3 of the user, identifying the user.

1 21. (New) The system of claim 17, further comprising a biometric
2 reader for generating a first biometric data of the user, wherein the
3 first biometric data of the user is compared with a second biometric
4 data of the user stored in the encrypted data file.

1 22. (New) The system of claim 17, further comprising a fingerprint
2 scanner for generating a first digitized fingerprint of the user, wherein
3 the first digitized fingerprint of the user is compared with a second
4 digitized fingerprint of the user stored in the encrypted data file.

1 23. (New) The system of claim 17, further comprising a server
2 configured to receive data encrypted using the authenticated encryption
3 key.

1 24. (New) A system for authenticating an encryption key of a user,
2 comprising:
3 _____ a input device for receiving a password provided by the user;
4 _____ an RF smart card for storing an encrypted data file, the data file
5 including an encryption key of the user;
6 _____ a decrypt engine for using the password to decrypt the encrypted
7 data file and thereby generate an authenticated encryption key of the
8 user; and
9 _____ memory for storing the decrypt engine.

1 25. (New) The system of claim 24, wherein the encrypted data file
2 includes encrypted biometric data identifying the user.

1 26. (New) The system of claim 24, wherein the encrypted data file
2 includes encrypted biometric data, derived from a digitized fingerprint of
3 the user, identifying the user.

1 27. (New) A system for authenticating an encryption key of a user,
2 comprising:

3 _____ a input device for receiving a password provided by the user;

4 _____ an RF smart card for storing an encrypted data file, the data file
5 including an encryption key of the user and a first biometric data of the
6 user;

7 _____ a biometric reader for generating a second biometric data of the
8 user; and

9 _____ a decrypt engine for using the password to decrypt the encrypted
10 data file, thereby generating an authenticated encryption key of the user,
11 if there is a probabilistic match between the first biometric data and the
12 second biometric data.

1 28. (New) A system for authenticating an encryption key of a user,
2 comprising:
3 _____ memory for storing an encrypted encryption key;
4 _____ an input device for receiving a password;
5 _____ a decrypt engine for using the password to decrypt the encrypted
6 encryption key to an authenticated decrypted encryption key; and
7 _____ memory for storing the decrypt engine.

1 29. (New) The system of claim 28, wherein the encrypted data file
2 includes encrypted biometric data identifying the user.

1 30. (New) The system of claim 28, wherein the encrypted encryption
2 key in is stored on an RF smart card.

1 31. (New) A system for authenticating an encryption key of a user,
2 comprising:
3 _____ memory for storing an encrypted encryption key and a first
4 biometric data of the user;
5 _____ an input device for receiving a password;
6 _____ a biometric reader for generating a second biometric data of the
7 user;
8 _____ a decrypt engine for comparing the first biometric data of the user
9 with a second biometric data of the user and, if there is a probabilistic
10 match, then using the password to decrypt the encrypted encryption key
11 to an authenticated decrypted encryption key; and
12 _____ memory for storing the decrypt engine.

1 32. (New) The system of claim 31, wherein the password is used to
2 decrypt the first biometric data before comparison with the second
3 biometric data.

4 33. (New) The system of claim 31, wherein the biometric reader is a
5 fingerprint scanner for generating a first digitized fingerprint of the user,
6 and the first biometric data is a digitized fingerprint of the user.

1 34. (New) A method for authenticating an encryption key of a user,
2 comprising the steps of:
3 storing an encrypted encryption key in memory;
4 receiving a password provided by a user; and
5 requiring use of the password to decrypt the encrypted
6 encryption key to a decrypted encrypting key.

1 35. (New) The method of claim 34, wherein the encrypted encryption
2 key is stored on an a RF smart card.

1 36. (New) The method of claim 34, wherein the encrypted encryption
2 key is stored with encrypted biometric data identifying the user.

1 37. (New) The method of claim 36, wherein the encrypted biometric
2 data includes a digitized fingerprint of the user.

1 38. (New) The system of claim 36, wherein the password is used to
2 decrypt the first biometric data before comparison with the second
3 biometric data.

1

1 39. (New) The method of claim 34, further comprising the steps of:
2 scanning a biometric feature of the user to generate first
3 biometric data of the user;
4 decrypting second biometric data stored along with the
5 encrypted encryption key;.
6 probabilistically comparing the generated first biometric data to
7 the decrypted second biometric data; and
8 requiring the comparison to produce a probabilistic match
9 before decrypting the encrypted encryption key to the decrypted
10 encryption key.

1 40. (New) The method of claim 32, further comprising the step of
2 reading the encrypted encryption key from an RF smart card.

1 41. (New) The method of claim 32, further comprising the step of
2 using the decrypted encryption key to encrypt data.